3 September 2025

Department of Home Affairs
Submitted via webform

Submission in response to the Government's Policy Discussion Paper *Charting New Horizons: developing Horizon 2 of the 2023-2030 Australian Cyber Security Strategy*.

auDA welcomes the opportunity to contribute to the consultation on Horizon 2 of the 2023–2030 Australian Cyber Security Strategy (Horizon 2).

We support the Strategy's shield-based approach and its emphasis on practical uplift of cyber security across the economy. Consistent with our previous submission to the Department of Home Affairs consultation on the 2023-2030 Australian Cyber Security Strategy, we reiterate our core positions: the importance of secure, reliable internet infrastructure and of multi-stakeholder collaboration.

Information about auDA's role and remit is attached at **Appendix 1.**

General comment

auDA congratulates the Department on the Government's implementation of the Strategy under Horizon 1: there has been good progress made, and significant initiatives completed since the Strategy was launched. The Horizon Two approaches set out in this paper will further advance the maturity of Australia's cyber security.

On the Cyber Security Policy Evaluation Model

auDA welcomes the approach set out in the paper, elaborated upon by the Department of Home Affairs in an online forum on 21 August 2025. Defining clear objectives and stating the intended causality between proposed (and current) interventions and the outcomes they are designed to deliver, is a welcome approach.

It will enhance the transparency of the Strategy's implementation and gives insights that will empower other stakeholders to contribute more effectively to achieving the key outcomes.

As the Department refines and develops the Model, it may be useful to develop a further level of detail, to drive in-depth understanding of the policy intent. A tiered metrics framework with regular review cycles and feedback loops would be suitable—for example, tracking the adoption of multi-factor authentication (MFA), safe-browsing

engagement and relevant domain name system (DNS) security indicators—to enable continuous improvement. This will further strengthen the ability of stakeholders to maximise their contributions.

auDA notes its *Digital Lives of Australians* research (most recently published in July 2025, and now spanning five years) as a potential source of insights and data that could be of use in the measurement aspects of the Model. Examples of relevant data from the 2025 report include:

- Reliance baseline: 64% of working Australians say they couldn't do their job without the internet[1]; 51% of small businesses say their business couldn't function without it, with 57% of regional small businesses rating the internet as "invaluable" to their function.[2]
- Security behaviour trend: Use of multi-factor authentication (MFA) rose to 73% in 2025, up from 55% in 2024.[3]
- Capability gap indicator: Only 20% of small businesses have a cyber security policy and just 18% audit their cyber security practices regularly.[4]

Comments relating to specific Shields

auDA offers the following comment in relation to Horizon 2 plans in relation to select Shield areas and consultation questions.

Shield 1 – Strong Businesses and Citizens

To better target and consolidate its cyber awareness message (Q5), Government could engage with industry and the education sector to jointly expand efforts to raise awareness on cyber security (for example through increased digital and in-person promotion at tertiary education providers, or social marketing to relevant early career professionals). Doing so could add significantly to improved awareness and penetration of key messages and improve Australia's baseline cyber literacy.

On standards for small and medium-sized businesses (SMBs) and not for profits (NFPs) (Q9), a practical "Essential Eight-light" pathway for resource-constrained SMEs/NFPs,

[1] *Digital Lives of Australians report* 2025, p. 9
[2] *Digital Lives of Australians report* 2025, p. 11
[3] *Digital Lives of Australians report* 2025, p. 23
[4] *Digital Lives of Australians report* 2025, p. 25

with clear model artefacts and optional independent assurance, may help drive the uplift. Grants or funding could be paired with such a standard to further support uplift compliance with the pathway. auDA has made a direct contribution to research in this area, with a recently-announced grant supporting research to enhance digital inclusion through strengthening vulnerable Australians' resilience to cyber scams.

Shield 2 – Safe Technology

On supporting consumers and end-users to be more informed about cyber security (Q 19), if it would be of value, auDA would be pleased to work with Government to produce a series of domain name security practice guides for domain name registrants, and other stakeholders in the domain name supply chain (alongside existing resources auDA has published). As a direct contribution in this Shield, auDA has announced grant funding to support research that will help assure a safe transition to a quantum-safe Domain Name System (DNS).

Shield 3 – World-Class Threat Sharing and Blocking

To drive industry block threats at scale (Qs 26, 28), a key contribution Government could make would be to consider creating a legislative basis that better supports industry collaboration such as threat sharing and blocking between sectors. This is relevant because regulatory mandates in other areas sometimes limit what can be shared (e.g. privacy legislation). Any such approach would be best designed in a very inclusive way to ensure its design avoids unintended impacts on other things valued by the community. auDA intends to convene Australian-based internet infrastructure stakeholders in 2026 to investigate how stronger collaboration can help tackle scams in this area.

Shield 4 – Protected Critical Infrastructure

To support critical infrastructure owners to mature their practice (Q36), a combination of access to cyber training and strategic use of the Department's audit rights under the SOCI Act could provide both capacity and incentive to support uplift. A wider set of examples and templates which smaller CI operators could more easily use in meeting CI obligations could also assist.

Shield 5 – Sovereign Capabilities

On Qs 39, 44 and 45, we note that auDA's 2025 *Digital Lives* research report identifies cyber security as a top future skill; 69% of working age Australians say cyber security skills are important for their current job or future career. Similarly, 81% of small businesses rate cyber security skills as important for their business. The research

reinforces that clear career pathways would be valued by the community. It also found that 70% of women don't feel they have the technical skills for a job in the technology industry. Australia could bolster its sovereign capabilities and ease the shortage of cyber security expertise by instigating government and industry collaboration on gender equity, promoting cyber security career options to girls in school, young women at university and to women seeking a mid-career transition. Options could include short, skills-focused training in cyber security, critical internet infrastructure operations, incident response and cyber security governance, delivered with industry and education partners.

Shield 6 – Strong Region and Global Leadership

The internet is no longer simply a communications network, but the backbone of the digital economy. It supports productivity, economic growth and social development by allowing Australian businesses to access global markets and Australian consumers to easily access goods, services and information from across the world.

The internet only works seamlessly across the globe due to its multistakeholder governance model, in which governments, the private sector, civil society and technical stakeholders collaborate on the standards, policies and processes that shape the internet's development.

We acknowledge Australia's longstanding commitment to multistakeholder internet governance. However, this model is highly contested, and we urge the Government to continue to support this commitment in the face of opposition.

To this end, continued dedicated resourcing and active Australian participation in the following forums and processes should be included as strategic priorities for Horizon 2 and beyond:

20-year review of the World Summit on the Information Society (WSIS+20)

This is a critical opportunity to shape the global digital development agenda and advocate for renewed commitment to multistakeholder internet governance and a renewed mandate for the Internet Governance Forum. Australia should continue its engagement in the WSIS process, including the twenty-year review and the implementation process.

International Telecommunication Union (ITU)

Australia should continue to participate in the ITU to influence global telecommunications standards and policies that shape the future of telecommunications and digital infrastructure. Active engagement by Government

ensures Australia's interests are represented in the global management of satellites and spectrum allocation and resist inappropriate scope creep of the ITU's mandate into critical internet resources (names, numbers and protocols).

auDA values the Government's continued engagement in all major ITU conferences including Plenipotentiary Conferences, the World Radio Conference, the World Telecommunications Development Conference and the World Telecommunications Standardisation Assembly. auDA also supports Australia seeking re-election to the ITU Council.

Asia Pacific Telecommunity (APT)

The APT fosters regional cooperation for development and expansion of infrastructure and services across the Asia Pacific. It also functions as a regional coordination group for preparing for major ITU conferences. Continued Government engagement is important to ensure Australian input is considered in the development of regional common positions.

Internet Corporation for Assigned Names and Numbers (ICANN)

Australian engagement in ICANN's Government Advisory Committee remains important as policies set at ICANN have potential to impact on national digital priorities including cyber security, competition and consumer protection.

Dedicated resourcing

Geopolitical uncertainty means Australian participation in global internet governance and digital policy processes is more urgent than ever to defend the interests of Australian businesses, consumers and internet users.

auDA acknowledges and commends the work of the staff at the Department of Infrastructure, Transport, Regional Development, Communications, Sport and the Arts in ICANN and the ITU and congratulate them for their significant contribution to thought leadership in their recent WSIS+20 non-paper. The ideas put forward in the paper have supported constructive multistakeholder dialogue and demonstrated Australia's capacity for global leadership.

We encourage the Government to continue to dedicate sustained resourcing to strengthening Australia's voice in global internet governance processes

While DTRDCSA is the lead agency for domestic and international internet governance, we also acknowledge the outstanding work of DFAT's cyber team. We hope the strategic

importance of diplomacy will continue to be recognised through the appointment of an experienced, trusted and influential cyber expert as Australia's next Cyber Ambassador.

For further information

If you would like to discuss our submission or any of the auDA research initiatives above, please contact auDA's Internet Governance and Policy Director, Jordan Carter, at jordan.carter@auda.org.au.

Dr. Bruce Tonkin
Chief Executive Officer

Appendix 1: About auDA

The .au Domain Administration Limited (auDA) is the trusted administrator of the .au country code Top Level Domain (ccTLD). The .au ccTLD is part of Australia's critical infrastructure, supporting more than 4.2 million .au domain names. auDA is endorsed by the Commonwealth Government to administer the .au for the benefit of all Australians under its Terms of Endorsement.

As a critical part of the digital economy, auDA's role is to ensure the .au ccTLD remains stable, reliable and secure. Additionally, auDA performs the following functions:

- Administering a licensing regime for .au domain names based in multi-stakeholder processes, including:
    - Developing policies for the .au domain with a multi-stakeholder approach to provide the greatest benefit for the Australian community.
    - Managing enquiries from the public about the licensing rules
    - Maintaining an appropriate compliance and dispute resolution process associated with the licensing rules
    - Making limited information available on the holder of a domain name licence through a publicly accessible tool at https://whois.auda.org.au/ (a standard feature of domain name systems around the world and an essential element of online accountability)
- Accrediting registrars to provide domain name registration services to the Australian internet community
- Advocating for, and actively participating in, multi-stakeholder internet governance processes both domestically and internationally.

In performing its functions, auDA operates under a multi-stakeholder model, working closely with the technical community, suppliers, business users, industry, civil society, consumers and the Australian Government.